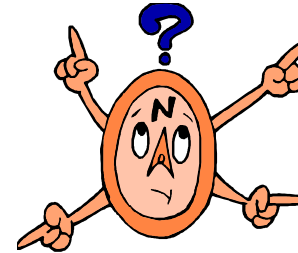# CJIS Online Overview

CJIS Security Awareness Training & Testing Software

Navigating the CJIS Online site

Working with the CJIS Online system:

- Logging in as a Local Agency Admin
- Setting up user accounts
- Modifying user accounts
- Relaying user login credentials & testing instructions
- Generating & reviewing test activity reports

CJIS Online is for level 1, 2 & 3 users

✦ It is the agency's responsibility to maintain CJIS Security Awareness training documentation.

✦ CJIS Security Awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.

If the person does not have a TLETS/Omnixx Login ID, they should be entered into CJIS Online:

- Level 1: Personnel that come in to contact with CJI
- Level 2: Personnel that enter, query or modify CJI
- Level 3: Personnel with Information Technology roles

CJIS Online is optional to Omnixx Level 2 personnel completing the Security Awareness Training in Omnixx.

All Personnel with CJI Access (Level 1)

Question: Who has physical access to CJI?

Answer: Anyone who has unescorted (eyes on it at all times) access to areas that process or store CJI.

Common examples include the following roles:

- Janitors
- Building maintenance
- Radio technician vendors
- Anyone given unfettered walking access to your secured location.

Personnel with Physical & Logical Access (Level 2)

Question: What does this mean?

Answer: Personnel with access to query, enter or modify CJI data.

Common examples include the following roles:

- Dispatchers
- Investigators
- Law enforcement officers

CJIS Online is optional to Omnixx Level 2 personnel completing the Security Awareness Training in Omnixx.

Personnel with Information Technology roles (Level **3**)

Question: What does this mean?

Answer: IT support staff with unescorted access to networking equipment such as: routers, switches, or servers processing, storing or transmitting CJI.

Access can be as simple as a key to the door that secures this equipment.

This can also be as complex as vendors with VPN access (unescorted) to systems that process CJI.

PLANNING AHEAD

✦ **START SMALL**
   enter staff without Omnixx/TLETS access that need training
   - IT staff and vendors

✦ **ADD Vendors**
   Create Vendor Admin account. Vendor Admins then enter their own employees

✦ As Omnixx/TLETS user accounts near expiration, enter them into CJIS Online

✦ CJIS Online requires a unique email address and Internet access for each person.

✦ Make a note of account login credentials created as you will be relaying this to users to start their training. Consider an email notification.

LOGIN TO THE CJIS ONLINE

Login to CJIS Online as an agency: https://www.cjisonline.com

If you cannot login,
512-424-7364
    or
**cjis.audit@
dps.texas.gov**

Agencies can set
only one admin for
CJIS online.

LOGIN TO THE CJIS ONLINE

Your login credentials are unique to you and the agency:

CJIS ONLINE – AGENCY OPTIONS

This is the agency's home screen listing all the options available to administer the agency, add/view vendors and run reports.

SETTING UP NEW CJIS ONLINE USERS

To add new users, click on "IT & Agency User Admin":

SETTING UP NEW CJIS ONLINE USERS

User accounts will be listed alphabetically

Add new users by clicking on the "Add New IT or Agency Employee" button:

SETTING UP NEW CJIS ONLINE USERS

Complete all mandatory fields marked by an asterisk *

Choose the appropriate training level 1,2 or 3 based on the level description.

Enter the person's unique email address & create a password.

This will become the initial user's sign on credential you will need to provide them.

Choose IT functions under categories, if applicable.

Level 2 TLETS operators may be currently covered under Omnixx security training and can be entered voluntarily.

Add IT or Agency Employee in Texas

Agency/ORI:	TX8888888
Department:	Maintenance *
State:	Texas
First Name:	Fred *
Middle Name:	
Last Name:	Flintstone *
Phone Number:	512-512-1212

Level Assignment

LEVEL NAME	LEVEL DESCRIPTION	ASSIGN
Level 1 CJIS Security Training	All Personnel with Access to CJI (This level is designed for people who do not have physical and logical access to CJI but may encounter it in their duties.)	◉
Level 2 CJIS Security Training	Personnel with Physical and Logical Access to CJI (This level is designed for operators who typically have access to query, enter, or modify CJI data.)	○
Level 3 CJIS Security Training	Personnel with Information Technology Roles (This level is designed for all information technology personnel including system administrators, security administrators, network administrator, etc.)	○

Finger Print Information
Date: [▼] [▼] [▼]

Email address is your user name

Email Address:	someone@emailaddress.com *
Confirm Email Address:	someone@emailaddress.com *
Password:	••••••••• *
Confirm Password:	••••••••• *

IT/Agency Related Categories

☐ Programming   ☐ Networking
☐ IT Management   ☐ Database Management
☐ Server Management   ☑ Support

[Submit] [Reset]

EDIT CJIS ONLINE USERS

Click on the magnifying glass to VIEW a record, edit credentials or inactivate.

Links on Page

***List All IT &
Agency
Employees***
**shows ACTIVE
users only**

***Show All
IT/Agency
Employees***
**displays ACTIVE
& INACTIVE
users**

EDIT CJIS ONLINE ACCOUNTS

Edit CJIS Online user training files with name changes, login credentials and add *optional* fingerprint information.

MANAGE VENDOR ADMIN ACCOUNTS

MANAGE VENDOR ACCOUNTS

Search by **Company Name**, Sort by **Category** or **State**. View & edit
records with the magnifying glass or notebook buttons.

Add a new vendor from this screen, if needed.

Many vendors are
preloaded into
the system.

- - - - - - - - - - - - -

! Perform an
extensive search
for a vendor
employee or
company name
first to prevent
creating duplicate
records.

Sample Email to user
to relay their login credentials

CJIS Security Awareness Training - Follow up required - Message (HTML)

From: Microsoft Exchange Server
To... firstname.lastname@emailaddress.com
Cc...
Bcc...
Subject: CJIS Security Awareness Training - Follow up required

Please complete the following CJIS Security Awareness Training before 01/01/2015.

To access the training, please go to https://www.cjisonline.com

Click on 'IT & AGENCY USERS' button.

Enter your user credentials:
Username: Firstname.lastname@emailaddress.com
Password: P@$$w0rd (Please note the password is case sensitive)

Once logged into the system, you may change your password.

Click on the 'TRAINING' button. You must read the ten training modules before taking the test.

After reading the training modules, return to the main menu.

Click on the 'TESTING' button.

Read the policy statement and click on the 'Confirm Training' box. You will have 1hour to take the 25 question test.

Take the test. To pass, you will need to achieve at least a 70 % (18 of 25 correct). This certification will be valid for two years after successfully completing. If you do not pass, you will need to wait at least one hour before taking the test again. There are no limitations on how many times to retake the test.

Once successfully complete, you may print your certificate if desired.

TAC

Staff and IT personnel sign on as "IT & Agency Users"

Vendor employees sign on as "Vendor Access"

TRAINING & TESTING

As directed in the email, after logging in the users will first complete the training modules then complete the test. Users must score at least 70% to pass the test and will have 1 hour to answer 18 of 25 questions correctly. If they do not pass the test they must wait 1 hour before trying again.

COMPLETION OF TRAINING & TESTING

Upon successful completion (70% or better) of the CJIS Online testing the user will receive a certificate. This user is now certified for two (2) years. Upon expiration the user will need to complete the training and testing process all over again – there is no recertification for CJIS Security Training.
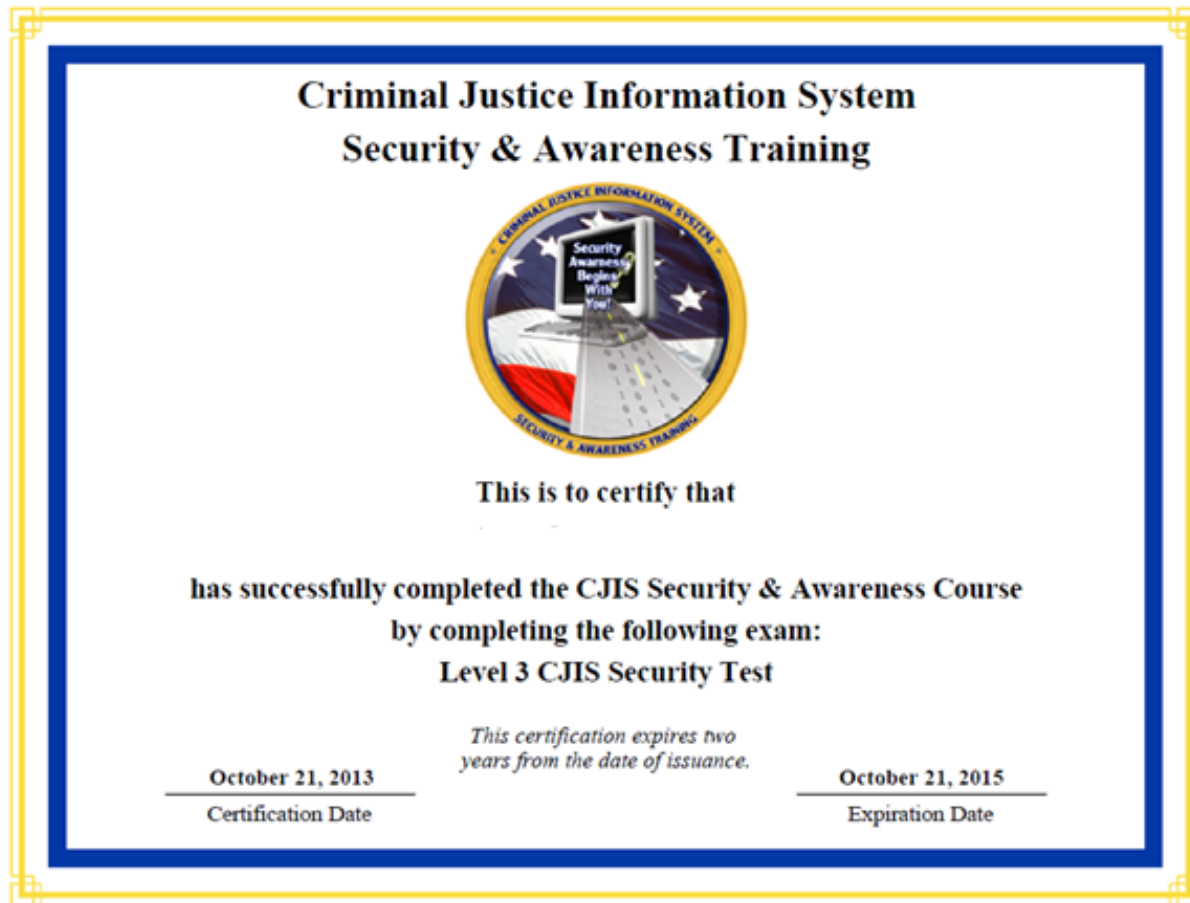
MONITORING TESTING ACTIVITY

Logging in as a "Local Agency Admin" you can run reports to monitor the agency's testing activity.

MONITORING TEST ACTIVITY

Regularly reviewing the Certification Expiration Report provides an agency wide perspective for upcoming expiration dates. Be proactive and administer training & testing reminders 60 days in advance to allow users time to complete the process.

CREATE AN EXPIRATION REPORT

This command will generate an expiration date list for the entire agency including active employees with no training history.

MONITOR AGENCY TESTING ACTIVITY

This report will list all dates in the database for the agency.
Pay special attention to the employees you have created accounts for but have not completed the necessary training.

CREATE A VENDOR EXPIRATION REPORT

This command will generate a specific vendor list with the expiration dates including those without training history.

MONITOR VENDOR TESTING ACTIVITY

This report lists the specific vendor selected with corresponding employee records.
Give special attention to any records expiring.
Vendor Admins are responsible for their own employees' training.

Questions?

Contact Info

If you cannot login,

512-424-7364

or

cjis.audit@dps.texas.gov